A covert authentication and security solution for GMOs

Significantly increasing worldwide utilization of genetically modified organisms (GMOs) presents challenges to ensure security, authenticity and validation of material goods and legal agreements. Similarly to the evolution witnessed in Internet protocols, strategic focus is required to anticipate, track and address potential infringements of GMO security. It is imperative that unimpeachable protocols assure product ownership, provide data to track the product supply chain, and to preempt malicious attacks especially related to bioagents. As GMOs are not tamper proof, it is necessary to encode and embed cyber-security data within the GMO genome in such a way as to allow a secure authentication process without revealing the signature to third parties.

Watermarking has been used extensively to establish authentication signatures that validate ownership by providing a mechanism to conceal and recover the required data necessary to authenticate the identification signature of the originator. However, in watermarking, the identity of the authentication information is disclosed as validity is verified. This leads to the risk of malicious transfer and signature duplication.

While some DNA embedding methods integrate several private and public key cryptographic algorithms, or encryption via a one-time pad, the cryptographic integration is only used for compression purposes of text data into binary. Previous methods focus on optimizing biocompatibility and practicality, in particular, on error detection and correction properties - not in the sense of cryptography - but inside the genome, to detect and correct mutations occurring during cell division that might destroy the information that is encrypted inside the genome. While the existing methods have benefited from numerous disciplines of digital communication theory, unique requirements of cryptography and security are first addressed in this work.

Although our work can be seamlessly combined with previous embedding methods, cryptographic aspect of GMOs requires additional tools and considerations. In contrast to correctness of encoding/decoding and efficiency, we consider the security aspects of a (digital) communication medium. As artificial DNA requires specific biocompatibility features and GMOs are not tamper proof, the security concerns of the DNA setting are unique. E.g., if someone were to produce a harmful bacterial clone carrying a specific watermark information, how would the originator of the watermark refute this clone was not theirs? Clearly, in the case of ownership watermarks, biocompatibility along with the correct and efficient encoding is not enough to address these and related concerns. Our protocol is provably secure in terms of standard cryptanalytic tools, yielding a highly secure and authentication-based product, which integrates a novel watermarking method and a probabilistic approach to address features like biocompatibility and concerns arising from cross-breeding.

A zero-knowledge (ZK) proof of knowledge of a hidden signature is used to build the designated confirmer signature. ZK proofs are both convincing and yet yield no information beyond the validity of the assertion being proved. A specific instantiation is described via the sign-then-encrypt

paradigm utilizing equality of discrete logarithms. Importantly, the signature is not transferrable. The crypto protocol, in combination with a new watermarking or data-embedding technique, embeds the authentication string indistinguishably from a random element in the signature space and the string is verified or denied without disclosing the actual signature. A focused adversary can only speculate whether a given sequence of nucleotides is a random sequence or a valid signature sequence. Results show that in a nucleotide string of 1000, the algorithm gives a correlation of 0.98 or higher between the distribution of the codon and that of E. coli, making the signature virtually invisible.

Siguna Mueller [1], ***Farhad Jafari*** [2], ***Don Roth*** [1]
[1]*Department of Molecular Biology, University of Wyoming, Laramie, WY, USA*
[2]*Department of Mathematics, University of Wyoming, Laramie, WY, USA*

Publication

A covert authentication and security solution for GMOs.
Mueller S, Jafari F, Roth D
BMC Bioinformatics. 2016 Sep 21